

General theory for decoy-state quantum key distribution with arbitrary number of intensities

Masahito Hayashi

ERATO-SORST Quantum Computation and Information Project, JST
5-28-3, Hongo, Bunkyo-ku, Tokyo, 113-0033, Japan

E-mail: masahito@qci.jst.go.jp

Abstract. We develop a general theory for quantum key distribution (QKD) in both the forward error correction and the reverse error correction cases when the QKD system is equipped with phase-randomized coherent light with arbitrary number of decoy intensities. For this purpose, generalizing Wang's expansion, we derive a convex expansion of the phase-randomized coherent state. We also numerically check that the asymptotic key generation rates are almost saturated when the number of decoy intensities is three.

PACS numbers: 03.67.Dd,03.67.Hk,03.67.-a,05.30.Jp

Keywords: decoy method, phase-randomized coherent state, key generation rate, arbitrary number of intensities

Submitted to: *New J. Phys.*

1. Introduction

The BB84 protocol proposed by Bennett and Brassard[1] has been known as a famous protocol guaranteeing information theoretical security. Its security has been proved by Mayers[2] in the single-photon case. However, implemented channels usually have imperfect quantum state generators, which generate not a perfect single-photon but a mixture of the vacuum state, the single-photon state, and the multi-photon state. In fact, many implemented quantum communication systems are equipped with phase-randomized weak coherent light, which can be regarded as the above type of mixed state[3, 4, 5, 6, 7]. In order to guarantee the security in the above imperfect quantum communication systems, Gottesman et al. (GLLP)[8], and Inamori et al. (ILM)[9] have obtained a useful formula for the asymptotic key generation (AKG) rate, which needs the counting rate and the phase error rate of single photon state. If we treat the worst case of these parameters, the obtained AKG rate become worse. In order to estimate these parameters properly, Hwang [10] proposed the decoy method, in which we randomly choose different intensities of the coherent light. In the decoy method, a pulse for final key generation is called the signal pulse while a pulse only for estimation of these parameters is called a decoy pulse. When k intensities are choosed for decoy pulses, we need to prepare $k + 1$ intensities. Therefore, as was pointed out by Lo et al.[11], for the estimation of the counting rate of single photon state, we have to treat an infinite number of the unknown parameters only with $k + 1$ equations even if the counting rates of individual number states do not depend on the basis. (Note that the counting rates for multi-photon states depend on the basis as well as the number of photon. However, we consider this special case for simplicity in introduction.) In this case, its estimate can be derived from the restriction for all unknown parameters. Hence, lager number of intensities yields a more precise estimate of the counting rate of single photon state. The phase error rate of single photon state has the same characterization.

In order to reduce the cost of its realization, Wang [12] proposed to choose the minimum decoy intensity to be the vacuum. By using this idea, QKD system can be implemented with k kinds of intensities essentially. In the following, we adopt this assumption. In the case of $k = 2$, Wang [12] also proposed an expansion of the phase-randomized coherent states $\sum_{n=0}^{\infty} \frac{e^{-\mu} \mu^n}{n!} |n\rangle \langle n|$, which describe the signal pulse and the decoy pulses. His expansion is different from the conventional expansion by number states in that the signal and decoy states can be described by stochastic mixtures of at most four states. Under his expansion, we obtain three constraint equations with four unknown parameters. He derived an estimate of the counting rate of the single photon state. Ma et al.[13] also derived the same estimate by a different method. Ma et al.[13] and Wang [14] obtained an estimate of the phase error rate of the single photon state, and completed the estimation of AKG rate in the case of $k = 2$, independently. Ma et al.[13] pointed out that if the second smallest intensity goes to 0, the required parameters can be solved perfectly. So, we obtain the best AKG rate, which is called the

universal upper bound‡. However, as was mentioned by them, it is impossible to control the infinitesimal intensity. Further, even if it is possible, if we choose small intensity, we cannot estimate the required parameters properly because the infinitesimal intensity makes our estimate fragile for statistical fluctuation. Thus, for a precise estimate, we need to fix the minimum difference between two intensities. That is, it is suitable to compare the qualities of our estimates by changing the number of decoy intensities under this constraint. For a good survey, please see Wang [15].

Now, we turn to the improvement of AKG rate. After GLLP-ILM's result, Lo[16] conjectured an improvement of their AKG rate with a rough idea of its proof. Based on his conjecture, Boileau-Batuwantudawe-Laflamme (BBL)[17] discussed a further improvement of the rate by taking into account the effects of dark counts in the detector. They pointed out that the AKG rate in the forward error correction case is different with respect to that in the reverse case. In the following, these rates will be called BBL formulas. Lo's conjecture has been proved by Hayashi [22] and Koashi [18], independently. Hence, it is suitable to apply these formulas to the decoy method.

In this paper, we treat the case of arbitrary number k of decoy intensities with BBL formulas when the intensity can be controlled§. For this purpose, we generalize Wang's expansion of the phase-randomized coherent states, in which $k + 1$ phase-randomized coherent states are given by convex combinations of $k + 2$ states, which are called *basis states*. The idea of this generalization is trivial, however, it is not trivial to derive the concrete forms of $k + 2$ basis states and to check their positivity. It is also needed to give the AKG rate formula by using the counting rates and the phase error rates of each intensities based on this expansion. For this purpose, we generalize mean value theorem and the concept of "difference". In the conventional mean value theorem, we treat the derivative of a given function f and the difference between outcomes of the function f in two points. In this paper, we extend the concept of "difference" to the case of $n + 1$ points, and derive its formula based on the n -th derivative. We also derive a formula for the generalized "difference". Using these formulas, we give concrete forms of $k + 2$ basis states and showed their positivity. We also derive a formula for estimating the counting rate and the phase error rate of the single photon state from the counting rates and the phase error rates of signal and decoy state. Then, the AKG rate formulas with BBL formulas are obtained. Moreover, we numerically compare the AKG rates of the cases of $k = 2, 3, 4$ and the universal upper bound in a proper model. As our result, the AKG rates of the case of $k = 3$ attain the universal upper bound within 1% error in case in the forward and reverse error case. That is, further great improvement cannot be expected even if the number k increases more than 3.

The organization of this paper is given as follows. Section 2 gives the AKG rates in both the forward and reverse cases as conjectured by BBL[17], taking into account

‡ Indeed, if we use a good code instead of random coding, there is a possibility to improve this bound. However, if we use random coding it is impossible to improve the universal upper bound.

§ For the case when the intensity fluctuates, see the papers [19, 20] and the back note [26] of the paper [21].

the effect of dark counts. In Section 3, we treat the universal upper bound in a proper channel model. In Section 4, we review the results by Wang [12, 14], Ma et al.[13]. In Section 5, we generalize Wang’s expansion of the phase-randomized coherent state $\sum_{n=0}^{\infty} \frac{e^{-\mu}\mu^n}{n!}|n\rangle\langle n|$. In Section 6, we give a lower bound of AKG rate based on the counting rates and phase error rates of respective intensities. In Section 7, we numerically compare the AKG rates in the case of $k = 2, 3, 4$ and its universal upper bound. In Section 8, the generalized “difference” is introduced, and all theorems are proved.

2. AKG rates with dark counts effect

When the transmitted pulse is given as a mixture of the vacuum, single-photon, and multi-photon, taking into account the effect of dark counts in the detector, BBL[17] conjectured the following AKG rate by use of Lo[16]’s conjecture, which is proved by Koashi [18] and Hayashi [22] with the threshold detector independently. Further, Hayashi [22] allows loss of detector if it is independent of the measurement basis. That is, we assume the same receiver model as Hayashi [22]. Let q^0 and q^1 be the probabilities detecting the the vacuum state and the single-photon state except for dark counts in detector. Let μ be the intensity of the signal pulse, which produces the raw keys. Then, We denote the dark count rate in the detector, the phase error rate concerning the single-photon state counted except for dark counts, the bit error probability of signal pulse, and the counting rate of signal pulse by p_D , r^1 , s_μ , and p_μ , respectively. When we use the phase-randomized coherent light with the intensity μ , $e^{-\mu}$ and $\mu e^{-\mu}$ are the probabilities generating the vacuum state and the single-photon state. In this case, Eve has no information concerning Bob’s bit of the pulses detected by dark counts and Alice’s bit of the pulses whose state is the vacuum state. Hence, the AKG rate with the forward error correction is different from that with the reverse error correction, and they are given as follows. (See BBL[17] or Section IV A of Hayashi[22].)

$$I_{\rightarrow} := \frac{1}{2} (\mu e^{-\mu} q^1 (1 - \bar{h}(r^1)) + e^{-\mu} (q^0 + p_D) - p_\mu \eta(s_\mu)) \quad (1)$$

$$I_{\leftarrow} := \frac{1}{2} (\mu e^{-\mu} q^1 (1 - \bar{h}(r^1)) + p_D - p_\mu \eta(s_\mu)), \quad (2)$$

where $\eta(s)$ is chosen so that $1 - \eta(s)$ is the coding rate of the classical error correction code and $\bar{h}(x)$ is given by

$$\bar{h}(x) = \begin{cases} -x \log_2 x - (1-x) \log_2(1-x) & \text{if } x \leq \frac{1}{2} \\ 1 & \text{if } x > \frac{1}{2}. \end{cases}$$

In the above formula, we regard the simultaneous event of a dark count and a normal count as a dark count. This is because the collision of both photons disturbs the information of the normal count.

These are the rates per one pulse sent by Alice. Thus, the coefficient $\frac{1}{2}$ corresponds to the probability that the basis of Alice coincides with that of Bob. For protocols attaining these rates, see Hayashi [22].

The dark count rate in the detector should be measured before the sending the quantum communication. In the above formulas, the parameters q^0, q^1 and r^1 are not known *a priori*. These cannot be estimated if only the pulse with the intensity μ is transmitted. In the decoy method [10], we randomly change the intensity μ and estimate these parameters from the counting rates and error rates of individual intensities. In particular, the parameter q^0 can be estimated by the counting rate p_0 of the vacuum pulses so that we obtain $q^0 = p_0 - p_D$. Once the parameter q^0 is fixed, both the AKG rates I_{\rightarrow} and I_{\leftarrow} are given as monotone increasing functions concerning $q^1(1 - \bar{h}(r^1))$. Hence, the remaining problem is the estimation of the parameters q^1 and r^1 , which is a more complicated problem.

In order to calculate these parameters, we need simultaneous equations concerning the individual intensities, in which the counting rates except for dark counts in detector and error rates of individual number states are treated as the unknown parameters. For simplicity, we assume that the counting rate except for dark counts in detector does not depend on the basis. Then, we let \tilde{q}^n be the counting rate of the state $|n\rangle\langle n|$, and \tilde{r}^n be the error rate of the state $|n\rangle\langle n|$ with the \times basis. Note that $\tilde{q}^1 = q^1$ and $\tilde{r}^1 = r^1$. Letting p_i be the counting rate of the intensity μ_i , and s_i be the error rate of the intensity μ_i with the \times basis, we obtain [11]

$$p_i = e^{-\mu_i}(p_0 - p_D) + e^{-\mu_i} \sum_{n=1}^{\infty} \frac{\mu_i^n}{n!} \tilde{q}^n + p_D \quad (3)$$

$$s_i p_i = e^{-\mu_i} \frac{1}{2}(p_0 - p_D) + e^{-\mu_i} \sum_{n=1}^{\infty} \frac{\mu_i^n}{n!} \tilde{r}^n \tilde{q}^n + \frac{1}{2} p_D \quad (4)$$

for $i = 1, \dots, k$ and

$$0 \leq \tilde{q}^n \leq 1, \quad 0 \leq \tilde{r}^n \leq 1. \quad (5)$$

That is, our task is to calculate the minimum value $I(\vec{p}, \vec{s})$ of $q^1(1 - \bar{h}(r^1))$ under the conditions (3), (4), and $1 - p_D \geq \tilde{q}^n \geq 0$, $1 \geq \tilde{r}^n \geq 0$, for given vectors $\vec{p} = (p_1, \dots, p_k)$ and $\vec{s} = (s_1, \dots, s_k)$.

3. Universal upper bounds on concrete noise model

In a real optical communication system, when the intensity is μ_i the dark counts rate in the optical fiber or the detector is p_0 , which is equal to the counting rate of the vacuum pulse, the counting rate p_i and the error rate s_i are given by

$$p_i = p_{i+k} = p(\mu_i) := 1 - e^{-\alpha\mu_i} + p_0 \quad (6)$$

$$s_i = s_{i+k} = s(\mu_i) := \frac{s(1 - e^{-\alpha\mu_i}) + \frac{1}{2}p_0}{p(\mu_i)}, \quad (7)$$

where the parameter α is the counting rate of the single photon except for dark counts in the detector or interfusion on optical fiber, and the parameter s is the error rate of single photon for normal detection. In an implemented channel, the parameter is

given by the function of the length of transmittance L as

$$\alpha = \theta \cdot 10^{-\frac{a_1 L + a_0}{10}}, \quad (8)$$

where θ is the efficiency of the detector, a_0 is loss coefficient in the detector, and a_1 is loss coefficient in the communication channel. When the detection probability of the n -photon state is $1 - (1 - \alpha)^n + p_0$, the relation (6) holds. When the error probability of the n -photon state is $\frac{s(1-(1-\alpha)^n)+\frac{1}{2}p_0}{1-(1-\alpha)^n+p_0}$, the relation (7) holds. Hence, the quantities $q^1 = \alpha + p_0 - p_D$ and $r^1 = \frac{s\alpha+\frac{1}{2}(p_0-p_D)}{\alpha+p_0-p_D}$ satisfy the conditions (3) and (4). Thus, we obtain

$$I(\vec{p}(\vec{\mu}), \vec{s}(\vec{\mu})) \leq (\alpha + (p_0 - p_D))(1 - \bar{h}(\frac{s\alpha + \frac{1}{2}(p_0 - p_D)}{\alpha + (p_0 - p_D)})),$$

where $\vec{p}(\vec{\mu}) = (p(\mu_1), \dots, p(\mu_k))$, $\vec{s}(\vec{\mu}) = (s(\mu_1), \dots, s(\mu_k))$. Therefore, applying (1) and (2), we obtain the following universal upper bounds of the AKG rates in the forward and reverse cases:

$$\begin{aligned} I_{\rightarrow}(\mu; p_0, p_D, \alpha, s) := & \frac{1}{2} \left[\mu e^{-\mu} (\alpha + (p_0 - p_D)) \left(1 - \bar{h} \left(\frac{s\alpha + \frac{1}{2}(p_0 - p_D)}{\alpha + (p_0 - p_D)} \right) \right) \right. \\ & \left. + e^{-\mu} p_0 - (1 - e^{-\alpha\mu} + p_0) \eta \left(\frac{s(1 - e^{-\alpha\mu}) + \frac{1}{2}p_0}{1 - e^{-\alpha\mu} + p_0} \right) \right] \end{aligned} \quad (9)$$

$$\begin{aligned} I_{\leftarrow}(\mu; p_0, p_D, \alpha, s) := & \frac{1}{2} \left[\mu e^{-\mu} (\alpha + (p_0 - p_D)) \left(1 - \bar{h} \left(\frac{s\alpha + \frac{1}{2}(p_0 - p_D)}{\alpha + (p_0 - p_D)} \right) \right) \right. \\ & \left. + p_D - (1 - e^{-\alpha\mu} + p_0) \eta \left(\frac{s(1 - e^{-\alpha\mu}) + \frac{1}{2}p_0}{1 - e^{-\alpha\mu} + p_0} \right) \right], \end{aligned} \quad (10)$$

respectively.

When $p_0 = p_D = 0$, both rates are equal to

$$\frac{1}{2}(\mu e^{-\mu} \alpha (1 - \bar{h}(s)) - (1 - e^{-\alpha\mu}) \bar{h}(s)),$$

which can be approximated by

$$\frac{1}{2}(\mu e^{-\mu} \alpha (1 - \bar{h}(s)) - (1 - e^{-\alpha\mu}) \bar{h}(s)) \cong \alpha \frac{\mu(e^{-\mu} - (1 + e^{-\mu})\bar{h}(s))}{2} \quad (11)$$

when α is sufficiently small.

As is shown in Appendix C, the optimum intensity is characterized as

$$\operatorname{argmax}_{\mu} I_{\rightarrow}(\mu; p_0, p_D, \alpha, s) \leq 1 \quad (12)$$

$$\operatorname{argmax}_{\mu} I_{\leftarrow}(\mu; p_0, p_D, \alpha, s) \leq 1. \quad (13)$$

If we choose intensities of decoy pulses suitably, the estimated parameters q^1 and r^1 are close to α and s . Hence, it is suitable to choose the intensity of the phase-randomized coherent light producing the raw keys among the interval $[0, 1]$.

4. Wang's expansion

We review the previous results concerning the estimation of the parameters q^1 and r^1 . In this section, we consider only the case of $p_D = 0$ because these results treated only this case. In order to avoid infinite number of unknown parameters in (3), Wang [12] proposed the following expansion of the states $\sum_{n=0}^{\infty} e^{-\mu_i} \frac{\mu_i^n}{n!} |n\rangle \langle n|$ in the case of $k = 2$:

$$\sum_{n=0}^{\infty} e^{-\mu_1} \frac{\mu_1^n}{n!} |n\rangle \langle n| = e^{-\mu_1} |0\rangle \langle 0| + e^{-\mu_1} \mu_1 |1\rangle \langle 1| + e^{-\mu_1} \mu_1^2 \Omega_2 \rho_2 \quad (14)$$

$$\sum_{n=0}^{\infty} e^{-\mu_2} \frac{\mu_2^n}{n!} |n\rangle \langle n| = e^{-\mu_2} |0\rangle \langle 0| + e^{-\mu_2} \mu_2 |1\rangle \langle 1| + e^{-\mu_2} \mu_2^2 \Omega_2 \rho_2 + e^{-\mu_2} \mu_2^2 (\mu_2 - \mu_1) \Omega_3 \rho_3, \quad (15)$$

where

$$\rho_2 := \frac{1}{\Omega_2} \sum_{n=2}^{\infty} \frac{\mu_1^{n-2}}{n!} |n\rangle \langle n|, \quad (16)$$

$$\rho_3 := \frac{1}{\Omega_3} \sum_{n=3}^{\infty} \frac{\mu_2^{n-2} - \mu_1^{n-2}}{(\mu_2 - \mu_1)n!} |n\rangle \langle n| \quad (17)$$

$$\Omega_2 := \frac{1}{\mu_1^2} (e^{\mu_1} - (1 + \mu_1)) \quad (18)$$

$$\Omega_3 := \frac{1}{\mu_2^2} (e^{\mu_2} - (1 + \mu_2 + \frac{\mu_2^2}{2})) - \frac{1}{\mu_1^2} (e^{\mu_1} - (1 + \mu_1 + \frac{\mu_1^2}{2})). \quad (19)$$

Based on this expansion, we define the parameters q^2, q^3, r^2 , and r^3 as

$$q^j := \text{Tr } \rho_j \sum_{n=2}^{\infty} \tilde{q}^n |n\rangle \langle n| \quad (20)$$

$$r^j q^j := \text{Tr } \rho_j \sum_{n=2}^{\infty} \tilde{q}^n \tilde{r}^n |n\rangle \langle n| \quad (21)$$

for $j = 2, 3$. Then, we have the following equations instead of (3) and (5):

$$p_1 = e^{-\mu_1} p_0 + e^{-\mu_1} \mu_1 q^1 + e^{-\mu_1} \mu_1^2 \Omega_2 q^2 \quad (22)$$

$$p_2 = e^{-\mu_2} p_0 + e^{-\mu_2} \mu_2 q^1 + e^{-\mu_2} \mu_2^2 \Omega_2 q^2 + e^{-\mu_2} \mu_2^2 (\mu_2 - \mu_1) \Omega_3 q^3 \quad (23)$$

$$0 \leq q^j \leq 1 \text{ for } j = 1, 2, 3. \quad (24)$$

Wang [12] gave a lower bound of q^2 in the following way. First, he calculated the maximum value q_U^2 of q^2 with the conditions (22), (23), and $q^1, q^3 \geq 0$:

$$q_U^2 = \frac{p_1}{\Omega_2} \left(\frac{1}{\mu_2 - \mu_1} \left(\frac{e^{-\mu_1} p_2}{\mu_2 e^{-\mu_2} p_1} - \frac{1}{\mu_1} \right) + \frac{e^{-\mu_1} p_0}{\mu_2 p_1} \right)$$

Using (22), he essentially obtained a lower bound $q_{2,\min}$ of q^1 :

$$q_{2,\min} := \frac{\mu_2 e^{\mu_1}}{\mu_1 (\mu_2 - \mu_1)} (p_1 - e^{-\mu_1} p_0) - \frac{\mu_1 e^{\mu_2}}{\mu_2 (\mu_2 - \mu_1)} (p_2 - e^{-\mu_2} p_0).$$

Wang [14] also obtained an upper bound $b_{1,\max}$ of $q^1 r^1$

$$b_{1,\max} := \frac{s_1 p_1 e^{\mu_1} - \frac{1}{2} p_0}{\mu_1}.$$

On the other hand, Ma et al. [13] treated the case where only two kinds of intensities are used for estimation of q^1 and r^1 . Their results can be translated into our case of $k = 3$ by putting the counting rate p_0 of the vacuum pulse into the parameter q^0 . Assume that $\mu_1 + \mu_2 < \mu_3$, $\mu_1 + \mu_2 < 1$, and $\mu_1 < \mu_2 < \mu_3$. Then, they obtained an lower bound of q^1 :

$$q^1 \geq q_L^{1,3} := \frac{\mu_3(p_2e^{\mu_2} - p_1e^{\mu_1} - \frac{\mu_2^2 - \mu_1^2}{\mu_3^2}(p_3e^{\mu_3} - p_0))}{\mu_2\mu_3 - \mu_3\mu_1 - \mu_2^2 + \mu_1^2}, \quad (25)$$

and an upper bound of q^1r^1 :

$$q^1r^1 \leq b_U^{1,2} := \frac{s_2p_2e^{\mu_2} - s_1p_1e^{\mu_1}}{\mu_2 - \mu_1}. \quad (26)$$

Taking the limit $\mu_1 \rightarrow 0$, they obtained the the lower bound $q_{2,\min}$ of q^1 in the case of $k = 2$. Also, similarly, they independently obtain the upper bound $b_{1,\max}$ of q^1r^1 .

Consider how tight the bounds $q_{2,\min}$ and $b_{1,\max}$ are. As will be mentioned in Theorem 2, the minimum value of q^1 under the conditions (22), (23) and $1 \geq q^2, q^3 \geq 0$ is calculated as

$$q_{\min}^{1,2} = \max\{q_{2,\min}, q_{1,\min}\},$$

where

$$q_{1,\min} := \frac{e^{\mu_1}}{\mu_1}(p_1 - e^{-\mu_1}p_0) - e^{-\mu_1}\mu_1^2\Omega_2.$$

Similar to (22) and (23), instead of (4), the relations

$$s_1p_1 = e^{-\mu_1}\frac{p_0}{2} + e^{-\mu_1}\mu_1q^1r^1 + e^{-\mu_1}\mu_1^2\Omega_2q^2r^2 \quad (27)$$

$$s_2p_2 = e^{-\mu_2}\frac{p_0}{2} + e^{-\mu_2}\mu_2q^1r^1 + e^{-\mu_2}\mu_2^2\Omega_2q^2r^2 + e^{-\mu_2}\mu_2^2(\mu_2 - \mu_1)\Omega_3q^3r^3 \quad (28)$$

$$0 \leq q^j r^j \leq 1 \text{ for } j = 1, 2, 3 \quad (29)$$

hold. Then, the maximum value $b_{\max}^{1,2}$ of q^1r^1 under the conditions (27), (28), and $1 \geq q^2r^2, q^3r^3 \geq 0$ is calculated as

$$b_{\max}^{1,2} = \min\{b_{1,\max}, b_{2,\max}\}$$

where

$$b_{2,\max} := \frac{\mu_2e^{\mu_1}}{\mu_1(\mu_2 - \mu_1)}(s_1p_1 - \frac{1}{2}e^{-\mu_1}p_0) - \frac{\mu_1e^{\mu_2}}{\mu_2(\mu_2 - \mu_1)}(s_2p_2 - \frac{1}{2}e^{-\mu_2}p_0 - e^{-\mu_2}\mu_2^2(\mu_2 - \mu_1)\Omega_3).$$

From (27), (28),

$$s_2p_2e^{\mu_2} - s_1p_1e^{\mu_1} = (\mu_2 - \mu_1)q^1r^1 + (\mu_2^2 - \mu_1^2)\Omega_2q^2r^2 + \mu_2^2(\mu_2 - \mu_1)\Omega_3q^3r^3.$$

Since $(\mu_2^2 - \mu_1^2)\Omega_2q^2r^2 \geq 0$ and $\mu_2^2(\mu_2 - \mu_1)\Omega_3q^3r^3 \geq 0$, we obtain $b_U^{1,3} \geq q^1r^1$. Hence, $b_U^{1,3} \geq b_{\max}^{1,2}$, i.e., the bound $b_{\max}^{1,2}$ is better than $b_U^{1,3}$.

Wang [14] proposed that the vacuum pulse and two kinds of intensities are used for estimating the parameters, and another intensity is used for signal pulse. In this method, it is possible to use the counting rate and the error rate of the signal pulse. Hence, it can be expected to improve the AKG rate by taking into account the the

counting rate and the error rate of the signal pulse. That is, it is needed to discuss the case of $k = 3$. In this case, Ma et al.'s bound $q_L^{1,3}$ can be applied. There is a possibility to improve existing bounds by extending Wang's expansion (14) and (15) to the case of $k = 3$. Further, as was pointed out by Ma et al.[13], we can expect that the AKG rates are close to the upper bounds $I_{\rightarrow}(\mu; p_0, p_D, \alpha, s)$ and $I_{\leftarrow}(\mu; p_0, p_D, \alpha, s)$ if the number k of intensities is sufficiently large. In the following section, we concentrate to derive better estimates of q^1 and $r^1 q^1$.

5. Convex expansion of mixed state $\sum_{n=0}^{\infty} \frac{e^{-\mu} \mu^n}{n!} |n\rangle \langle n|$

5.1. Extension of Wang's expansion

In this section, we give a convex expansion of the phase-randomized coherent state $\sum_{n=0}^{\infty} \frac{e^{-\mu} \mu^n}{n!} |n\rangle \langle n|$ as an extension of Wang's expansion (14) and (15):

Theorem 1 Assume that $\mu_1 < \dots < \mu_k$. Define the basis state ρ_i ($i = 2, \dots, k+1$) as

$$\begin{aligned}\rho_i &:= \frac{1}{\Omega_i} \sum_{n=i}^{\infty} \frac{\gamma_{i,n}}{n!} |n\rangle \langle n|, \\ \gamma_{i,n} &:= \sum_{j=1}^{i-1} \frac{\mu_j^{n-2}}{\prod_{t=1, t \neq j}^{i-1} (\mu_j - \mu_t)} \\ \Omega_i &:= \sum_{n=i}^{\infty} \frac{\gamma_{i,n}}{n!}.\end{aligned}$$

Then, ρ_i is positive semi-definite, and

$$e^{-\mu_i} \sum_{n=0}^{\infty} \frac{\mu_i^n}{n!} |n\rangle \langle n| = e^{-\mu_i} \left(|0\rangle \langle 0| + \mu_i |1\rangle \langle 1| + \sum_{n=2}^{i+1} \mu_i^2 \prod_{t=1}^{n-2} (\mu_i - \mu_t) \Omega_n \rho_n \right) \quad (30)$$

Note that the coefficient $\mu_i^2 \prod_{t=1}^{n-2} (\mu_i - \mu_t) \Omega_n$ is positive.

The quantities Ω_2 and Ω_3 coincide with those defined in (18) and (19). Hence, we can check that the above expansion of the case of $k = 2$ reproduces Wang's expansion (14) and (15). Further, Ω_4 and Ω_5 are calculated as

$$\begin{aligned}\Omega_4 &= \frac{1}{\mu_3^2(\mu_3 - \mu_1)} (e^{\mu_3} - 1 - \mu_3 - \frac{\mu_3^2}{2} - \frac{\mu_3^3}{6}) - \frac{1}{\mu_2^2(\mu_2 - \mu_1)} (e^{\mu_2} - 1 - \mu_2 - \frac{\mu_2^2}{2} - \frac{\mu_2^3}{6}) \\ &\quad + \frac{1}{\mu_1^2(\mu_2 - \mu_1)} (e^{\mu_1} - 1 - \mu_1 - \frac{\mu_1^2}{2} - \frac{\mu_1^3}{6})\end{aligned}$$

and

$$\begin{aligned}\Omega_5 &= \frac{1}{\mu_4^2(\mu_4 - \mu_2)(\mu_4 - \mu_1)} (e^{\mu_4} - 1 - \mu_4 - \frac{\mu_4^2}{2} - \frac{\mu_4^3}{6} - \frac{\mu_4^4}{24}) \\ &\quad - \frac{1}{\mu_3^2(\mu_3 - \mu_2)(\mu_3 - \mu_1)} (e^{\mu_3} - 1 - \mu_3 - \frac{\mu_3^2}{2} - \frac{\mu_3^3}{6} - \frac{\mu_3^4}{24})\end{aligned}$$

$$\begin{aligned}
& + \frac{1}{\mu_2^2(\mu_3 - \mu_2)(\mu_2 - \mu_1)} (e^{\mu_2} - 1 - \mu_2 - \frac{\mu_2^2}{2} - \frac{\mu_2^3}{6} - \frac{\mu_2^4}{24}) \\
& - \frac{1}{\mu_1^2(\mu_3 - \mu_1)(\mu_2 - \mu_1)} (e^{\mu_1} - 1 - \mu_1 - \frac{\mu_1^2}{2} - \frac{\mu_1^3}{6} - \frac{\mu_1^4}{24}).
\end{aligned}$$

In order to estimate the parameters q^1 and r^1 , we introduce new parameters q^2, \dots, q^{k+1} , and r^2, \dots, r^{k+1} by

$$q^j := \text{Tr } \rho_j \sum_{n=2}^{\infty} \tilde{q}^n |n\rangle \langle n| \quad (31)$$

$$r^j q^j := \text{Tr } \rho_j \sum_{n=2}^{\infty} \tilde{q}^n \tilde{r}^n |n\rangle \langle n| \quad (32)$$

for $j = 2, \dots, k+1$. Hence, instead of (3) and (4), as a generalization of (22), (23), (27), and (28) we obtain the equations:

$$\begin{aligned}
p_i &= \sum_{j=0}^{k+1} P'_i{}^j q^j, \\
s_i p_i &= \sum_{j=1}^{k+1} P'_i{}^j q^j r^j + \frac{1}{2} P'_i{}^0 q^0,
\end{aligned}$$

for $i = 1, 2, \dots, k$, where

$$P' := \begin{pmatrix} 1 & 0 & 0 \\ Y & Z & X \end{pmatrix},$$

and the k -dimensional vectors Y and Z and the $k \times k$ matrix X are given by

$$\begin{aligned}
Y_i &:= e^{-\mu_i} \\
Z_i &:= \mu_i e^{-\mu_i} \\
X_i^j &:= \begin{cases} \mu_i^2 \prod_{t=1}^{j-1} (\mu_i - \mu_t) e^{-\mu_i} \Omega_{j+1} & \text{if } j = 1, \dots, i \\ 0 & \text{if } j = i+1, \dots, k \end{cases}
\end{aligned}$$

for $i = 1, \dots, k$.

5.2. General case

In the previous subsection, we treat the case where $p_D = 0$ and the counting rates and the error rates of the \times basis are equal to those of the $+$ basis. Since the average state of the state ρ_j with the \times basis is different from that the $+$ basis, we have to treat the parameter q^{j+k} of the $+$ basis as a parameter different from the parameter q^j of the \times basis in the general setting. In this subsection, we extend the discussion of the above subsection to the general case. Let \tilde{q}_x^n and \tilde{r}_x^n be the counting rate except for dark counts in detector and error rate of the number state $|n\rangle \langle n|$ with the \times basis, and \tilde{q}_+^n and \tilde{r}_+^n be those with the $+$ basis. Instead of (31) and (32), the parameters q^2, \dots, q^{2k+1} ,

and r^2, \dots, r^{k+1} are introduced by

$$q^j := \text{Tr } \rho_j \sum_{n=2}^{\infty} \tilde{q}_x^n |n\rangle\langle n| \quad (33)$$

$$q^{j+k} := \text{Tr } \rho_j \sum_{n=2}^{\infty} \tilde{q}_+^n |n\rangle\langle n| \quad (34)$$

$$r^j q^j := \text{Tr } \rho_j \sum_{n=2}^{\infty} \tilde{q}_x^n \tilde{r}_x^n |n\rangle\langle n| \quad (35)$$

for $j = 2, \dots, k+1$. That is, the upper index j has the following meaning:

$j = 0$: The vacuum state

$j = 1$: The single-photon state

$j = 2, \dots, k+1$: The state ρ_j with the \times basis

$j = k+2, \dots, 2k+1$: The state ρ_{j-k} with the \times basis

Note that q^j is the rate of counting except for dark counts. Instead of (33) – (35), we have the relations

$$p_i = \sum_{j=0}^{2k+1} P_i^j q^j + p_D, \quad (36)$$

for $i = 0, \dots, 2k$, and

$$s_i p_i = \sum_{j=1}^{k+1} P_i^j q^j r^j + \frac{1}{2}(P_i^0 q^0 + p_D), \quad (37)$$

for $i = 1, 2, \dots, k$. In addition, r^i belongs to $[0, 1]$ for $i = 1, \dots, k$, and q^i belongs to $[0, 1 - p_D]$ for $i = 0, \dots, 2k+1$ because the dark counts occur with the probability p_D . Therefore, we can estimate of the ranges of q^1 and r^1 from these conditions. Here, we defined the matrix $(P_i^j)_{i=0, \dots, 2k, j=0, \dots, 2k+1}$ defined by

$$P := \begin{pmatrix} 1 & 0 & 0 & 0 \\ Y & Z & X & 0 \\ Y & Z & 0 & X \end{pmatrix},$$

where the k -dimensional vectors Y and Z and the $k \times k$ matrix X are given the above.

For examples, this matrix in the case of $k = 1, 2, 3$ is given as

$$P_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ e^{-\mu_1} & \mu_1 e^{-\mu_1} & e^{-\mu_1} \mu_1^2 \Omega_2 & 0 \\ e^{-\mu_1} & \mu_1 e^{-\mu_1} & 0 & e^{-\mu_1} \mu_1^2 \Omega_2 \end{pmatrix},$$

$$P_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ e^{-\mu_1} & \mu_1 e^{-\mu_1} & e^{-\mu_1} \mu_1^2 \Omega_2 & 0 & 0 & 0 \\ e^{-\mu_2} & \mu_2 e^{-\mu_2} & e^{-\mu_2} \mu_2^2 \Omega_2 & e^{-\mu_2} \mu_2^2 (\mu_2 - \mu_1) \Omega_3 & 0 & 0 \\ e^{-\mu_1} & \mu_1 e^{-\mu_1} & 0 & 0 & e^{-\mu_1} \mu_1^2 \Omega_2 & 0 \\ e^{-\mu_2} & \mu_2 e^{-\mu_2} & 0 & 0 & e^{-\mu_1} \mu_2^2 \Omega_2 & e^{-\mu_2} \mu_2^2 (\mu_2 - \mu_1) \Omega_3 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ e^{-\mu_1} & \mu_1 e^{-\mu_1} & e^{-\mu_1} \mu_1^2 \Omega_2 & 0 & 0 & 0 & 0 & 0 \\ e^{-\mu_2} & \mu_2 e^{-\mu_2} & e^{-\mu_2} \mu_2^2 \Omega_2 & e^{-\mu_2} \mu_2^2 (\mu_2 - \mu_1) \Omega_3 & 0 & 0 & 0 & 0 \\ e^{-\mu_3} & \mu_3 e^{-\mu_3} & e^{-\mu_3} \mu_3^2 \Omega_2 & e^{-\mu_3} \mu_3^2 (\mu_3 - \mu_1) \Omega_3 & * & 0 & 0 & 0 \\ e^{-\mu_1} & \mu_1 e^{-\mu_1} & 0 & 0 & 0 & e^{-\mu_1} \mu_1^2 \Omega_2 & 0 & 0 \\ e^{-\mu_2} & \mu_2 e^{-\mu_2} & 0 & 0 & 0 & e^{-\mu_2} \mu_2^2 \Omega_2 & e^{-\mu_2} \mu_2^2 (\mu_2 - \mu_1) \Omega_3 & 0 \\ e^{-\mu_3} & \mu_3 e^{-\mu_3} & 0 & 0 & 0 & e^{-\mu_3} \mu_3^2 \Omega_2 & e^{-\mu_3} \mu_3^2 (\mu_3 - \mu_1) \Omega_3 & * \end{pmatrix}$$

where

$$* = e^{-\mu_3} (\mu_3 - \mu_1) (\mu_3 - \mu_2) \Omega_4.$$

6. Asymptotic key generation (AKG) rates

In this section, based on the expansion (30), we derive a lower bound of $I(\vec{p}, \vec{s})$. Since the matrix P_i^j has no inverse matrix, it is impossible to derive q^1 and r^1 from the conditions (36) and (37) uniquely. Then, in order to evaluate $I(\vec{p}, \vec{s})$, we introduce the quantities $q_{\min}^{1,k}$ and $b_{\max}^{1,k}$ by

$$q_{\min}^{1,k} := \min_{\vec{q}=(q^0, \dots, q^{2k+1})^T} \left\{ q^1 \middle| \begin{array}{l} p_i = \sum_{j=0}^{2k+1} P_i^j q^j + p_D \\ 1 - p_D \geq q^0, \dots, q^{2k+1} \geq 0 \end{array} \right\}$$

$$b_{\max}^{1,k} := \max_{\vec{b}=(b^1, \dots, b^{k+1})^T} \left\{ b^1 \middle| \begin{array}{l} s_i p_i = \sum_{j=1}^{k+1} P_i^j b^j \\ + \frac{P_i^0 (p_0 - p_D) + p_D}{2} \\ 1 - p_D \geq b^1, \dots, b^{k+1} \geq 0 \end{array} \right\}$$

for $i = 0, \dots, k$. Then, the minimum value $I(\vec{p}, \vec{s})$ can be evaluated by

$$q_{\min}^{1,k} \left(1 - \overline{h}\left(\frac{b_{\max}^{1,k}}{q_{\min}^{1,k}}\right) \right) \leq I(\vec{p}, \vec{s}).$$

Thus, when μ_k is the signal intensity,

$$\begin{aligned} \frac{1}{2} (\mu_k e^{-\mu_k} I(\vec{p}, \vec{s}) + e^{-\mu_k} (q^0 + p_D) - p_{\mu_k} \eta(s_{\mu_k})) &\leq I_{\rightarrow} \\ \frac{1}{2} (\mu_k e^{-\mu_k} I(\vec{p}, \vec{s}) + p_D - p_{\mu_k} \eta(s_{\mu_k})) &\leq I_{\leftarrow}. \end{aligned}$$

In the following, we calculate $b_{\max}^{1,k}$ and $q_{\min}^{1,k}$ as follows.

Theorem 2 Define the quantities $q_{j,\min}$, $q_{k+j,\min}$, and $b_{j,\max}$ by

$$q_{j,\min} := \begin{cases} \sum_{i=1}^j \beta_i^j (p_i - p_D - e^{-\mu_i} (p_0 - p_D)) - (1 - p_D) \mu_1 \cdots \mu_j \Omega_{j+1} & \text{if } j \text{ is odd.} \\ \sum_{i=1}^j \beta_i^j (p_i - p_D - e^{-\mu_i} (p_0 - p_D)) & \text{if } j \text{ is even.} \end{cases} \quad (38)$$

$$q_{k+j,\min} := \begin{cases} \sum_{i=1}^j \beta_i^j (p_{i+k} - p_D - e^{-\mu_i} (p_0 - p_D)) - (1 - p_D) \mu_1 \cdots \mu_j \Omega_{j+1} & \text{if } j \text{ is odd} \\ \sum_{i=1}^j \beta_i^j (p_{i+k} - p_D - e^{-\mu_i} (p_0 - p_D)) & \text{if } j \text{ is even.} \end{cases} \quad (39)$$

$$b_{j,\max} := \begin{cases} \sum_{i=1}^j \beta_i^j (s_i p_i - \frac{1}{2} (p_D + e^{-\mu_i} (p_0 - p_D))) & \text{if } j \text{ is odd} \\ \sum_{i=1}^j \beta_i^j (s_i p_i - \frac{1}{2} (p_D + e^{-\mu_i} (p_0 - p_D))) + (1 - p_D) \mu_1 \cdots \mu_j \Omega_{j+1} & \text{if } j \text{ is even.} \end{cases} \quad (40)$$

$$\beta_i^j := (-1)^{j-1} \frac{\mu_1 \cdots \mu_j e^{\mu_i}}{\mu_i^2 \prod_{t=1, t \neq i}^j (\mu_t - \mu_i)} \quad (41)$$

for $j \leq k$. Then, the relations

$$q_{j,\min} = \min_{\vec{q}=(q^0, \dots, q^{2k+1})^T} \left\{ q^1 \mid \begin{array}{l} p_i = \sum_{j=0}^{2k+1} P_i^j q^j + p_D \\ 1 - p_D \geq q^{1+j} \geq 0 \end{array} \right\} \quad (42)$$

$$q_{k+j,\min} = \min_{\vec{q}=(q^0, \dots, q^{2k+1})^T} \left\{ q^1 \mid \begin{array}{l} p_i = \sum_{j=0}^{2k+1} P_i^j q^j + p_D \\ 1 - p_D \geq q^{1+j+k} \geq 0 \end{array} \right\} \quad (43)$$

$$b_{j,\max} = \max_{\vec{b}=(b^1, \dots, b^{k+1})^T} \left\{ b^1 \mid \begin{array}{l} s_i p_i = \sum_{j=1}^{k+1} P_i^j b^j + \frac{P_i^0(p_0 - p_D) + p_D}{2} \\ 1 - p_D \geq b^{1+j} \geq 0 \end{array} \right\}, \quad (44)$$

hold. Therefore, $q_{\min}^{1,k}$ and $b_{\max}^{1,k}$ are calculated as

$$q_{\min}^{1,k} = \max\{q_{1,\min}, \dots, q_{2k,\min}\} \quad (45)$$

$$b_{\max}^{1,k} = \min\{b_{1,\max}, \dots, b_{k,\max}\}. \quad (46)$$

In order to calculate $q_{j,\min}$ and $b_{j,\max}$ in the channel model (6) and (7), we define the quantity $\epsilon_\alpha^j(\mu_1, \dots, \mu_j)$:

$$\epsilon_\alpha^j(\mu_1, \dots, \mu_j) := (-1)^{j-1} \left(\sum_{i=1}^j \beta_i^j (1 - e^{-\alpha \mu_i}) - \alpha \right) \geq 0. \quad (47)$$

This quantity can be characterized by the following theorem.

Theorem 3 We denote the $j-1$ -dimensional simplex and its uniform probability measure by Δ_{j-1} and p_{j-1} , respectively. Then, $\epsilon_\alpha^j(\mu_1, \dots, \mu_j)$ is characterized as follows.

$$\epsilon_\alpha^j(\mu_1, \dots, \mu_j)$$

$$= \frac{\mu_1 \cdots \mu_j}{(j-1)!} \int_{\Delta_{j-1}} \sum_{n=0}^{\infty} \frac{1 - (1-\alpha)^{n+j+1}}{(n+j+1)(n+j)n!} \left(\sum_{i=1}^j a_i \mu_i \right)^n p_{j-1}(a_1 \dots a_j) da_1 \dots da_j \quad (48)$$

$$= \mu_1 \cdots \mu_j \sum_{n=j+1}^{\infty} \sum_{i_l \geq 0: i_1 + \dots + i_j = n-1-j} \frac{1}{n!} (1 - (1-\alpha)^n) \mu_1^{i_1} \cdots \mu_j^{i_j}. \quad (49)$$

Ω_{j+1} is calculated as

$$\mu_1 \cdots \mu_j \Omega_{j+1} = \epsilon_1^j(\mu_1, \dots, \mu_j). \quad (50)$$

Using the relations (47) and (50), we can calculate $q_{j,\min}$, $q_{k+j,\min}$, and $b_{j,\max}$ in the channel model (6) and (7) as follows:

$$q_{j,\min} = q_{k+j,\min} \begin{cases} \alpha + (p_0 - p_D) + \epsilon_\alpha^j(\mu_1, \dots, \mu_j) - (1-p_0)\epsilon_1^j(\mu_1, \dots, \mu_j) & \text{if } j \text{ is odd.} \\ \alpha + (p_0 - p_D) - \epsilon_\alpha^j(\mu_1, \dots, \mu_j) - (p_0 - p_D)\epsilon_1^j(\mu_1, \dots, \mu_j) & \text{if } j \text{ is even.} \end{cases}$$

$$b_{j,\max} = \begin{cases} s\alpha + \frac{1}{2}(p_0 - p_D) + s\epsilon_\alpha^j(\mu_1, \dots, \mu_j) + \frac{p_0 - p_D}{2}\epsilon_1^j(\mu_1, \dots, \mu_j) & \text{if } j \text{ is odd.} \\ s\alpha + \frac{1}{2}(p_0 - p_D) - s\epsilon_\alpha^j(\mu_1, \dots, \mu_j) + (1 - \frac{1}{2}(p_0 + p_D))\epsilon_1^j(\mu_1, \dots, \mu_j) & \text{if } j \text{ is even.} \end{cases}$$

From the expression (48), $\epsilon_\alpha^j(\mu_1, \dots, \mu_j)$ is monotone increasing concerning all of μ_1, \dots, μ_j , and α . Also the expression (48) implies that $\epsilon_\alpha^j(\mu_1, \dots, \mu_j)$ goes to 0 when μ_1 goes to 0. That is, the upper bounds $I_{\rightarrow}(\mu; p_0, p_D, \alpha, s)$ and $I_{\leftarrow}(\mu; p_0, p_D, \alpha, s)$ can be attained. This fact coincides with the fact that $\tilde{q}_L^{1,2}$ goes to s when μ_1 goes to 0,

which was proved by Ma et al.[13]. However, in a realistic system, it is impossible to take the limit $\mu_1 \rightarrow 0$. Even if, we could realize such a small μ_1 , the estimation process is not robust for statistical fluctuation. Hence, in order to attain the upper bounds $I_{\rightarrow}(\mu; p_0, p_D, \alpha, s)$ and $I_{\leftarrow}(\mu; p_0, p_D, \alpha, s)$, it is suitable to fix the minimum of the width $\mu_i - \mu_{i-1}$ and increase the number k .

7. Comparison of AKG rates

In order to compare estimates of q^1 and q^1r^1 , we assume that $p_i = p_{i+k}$. As is mentioned in Section 4, $q_{\min}^{1,2}$ and $b_{\max}^{1,2}$ give the best estimates of q^1 and q^1r^1 among known estimates in the case of $k = 2$.

In this section, we assume the channel model (6)-(8). As a typical case, we focus on the case of $a_1 = 0.17$ dB/km, which is the lowest loss values in commercially available optical fibres[23] $a_0 = 5$ dB, $\theta = 0.1$, $p_0 = 4.0 \times 10^{-7}$, $s = 0.03$ [4].

The minimum of the width $\mu_i - \mu_{i-1}$ is 0.1. For simplicity, we assume that our code of classical error correction attains the Shannon rate.

Now, we compare the AKG rates with the forward error correction with existing estimates. For fair comparison, we do not take into account the dark count effect, i.e., assume that $p_D = 0$. Then, we calculate the following values as functions of the distance L :

- (2) $\max_{0.2 < \mu_2} I(\mu_2, q_{2,\min}(0.1, \mu_2), b_{1,\max}(0.1))$. Ma et al.[13], Wang[14]
- (3.1) $\max_{0.3 < \mu_3} I(\mu_3, q_L^{1,3}(0.1, 0.2, \mu_3), b_{1,\max}(0.1))$. Ma et al.[13]
- (3.2) $\max_{0.3 < \mu_3} I(\mu_3, q_{2,\min}(0.1, 0.2), b_{1,\max}(0.1))$. Wang[14] $k = 3$
- (3.3) $\max_{0.3 < \mu_3} I(\mu_3, q_{\min}^{1,3}(0.1, 0.2, \mu_3), b_{\max}^{1,3}(0.1, 0.2, \mu_3))$. Our result $k = 3$
- (4) $\max_{0.4 < \mu_4} I(\mu_4, q_{\min}^{1,4}(0.1, 0.2, 0.3, \mu_4), b_{\max}^{1,4}(0.1, 0.2, 0.3, \mu_4))$. Our result $k = 4$
- (5) $\max_{0 < \mu} I(\mu, \alpha - p_0 + p_D, s\alpha + \frac{1}{2}(p_0 - p_D))$. Upper bound

Here, in order to treat the forward error correction case with $p_D = 0$, we put $I(\mu, q^1, b^1)$ as $I(\mu, q^1, b^1) := \frac{1}{2}(\mu e^{-\mu} q^1(1 - h(\frac{b^1}{q^1})) + e^{-\mu} p_0 - p(\mu)h(s(\mu)))$. In this case, we can numerically check that $q_{\min}^{1,2} = q_{2,\min}$, $q_{\min}^{1,3} = q_{2,\min}$, $q_{\min}^{1,4} = q_{4,\min}$, $b_{\max}^{1,2} = b_{1,\max} < b_U^{1,2}$, $b_{\max}^{1,3} = b_{3,\max}$, $b_{\max}^{1,4} = b_{3,\max}$. Here, we treat $q_L^{1,3}$, $q_L^{1,2}$, $q_{2,\min}$, $q_{\min}^{1,3}$, $b_{1,\max}$, $b_{\max}^{1,3}$, as functions of μ_1, μ_2 , (μ_3, μ_4) with the model (6), (7). The transmission rates of the above six cases are given in the Fig 1. The achievable transmission length is (2)222.8km, (3.1)215.2km, (3.2)223.2km, (3.3)224.5km, (4)224.8km, (5)225.2km. That is, by increasing the number k from 2 to 3 yields increasing the achievable transmission length increases with 1.7 km, while increasing the number k from 3 to the infinity yields increasing it only with 0.7 km.

Next, taking into account the dark count effect, we consider the effect of increase of the number k of intensities with the forward and reverse error correction. In these comparisons, it is assumed that all detections with the vacuum pulse are caused by the dark count effect in the detector, i.e., $p_D = p_0$.

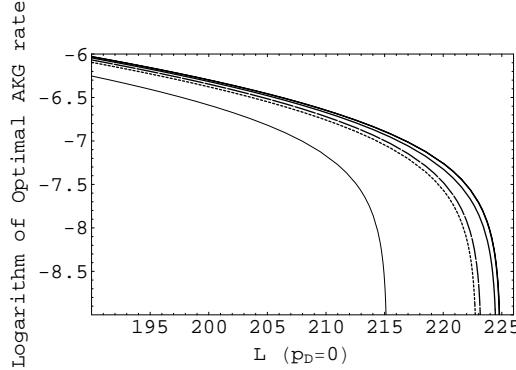


Figure 1. The transmission rate ($p_D = 0$): From left to right, (3.1), (2), (3.2), (3.3), (4), (5). We cannot distinguish (4) and (5) in this graph.

In order to discuss the forward error correction case with $p_D = p_0$, we replace the definitions of $q_{2,\min}$, $b_{1,\min}$, $q_{\min}^{1,3}$, $b_{\min}^{1,3}$, $q_{\min}^{1,4}$, and $b_{\min}^{1,4}$ in the above table because these depend on the value p_D . The transmission rates of the five cases (2), (3.2), (3.3), (4), and (5) with the forward error correction are given in the Fig 2. The achievable transmission length in the forward case is (2)223.0km, (3.2)223.5km, (3.3)224.5km, (4)224.8km, (5)225.2km. That is, increasing the number k from 2 to 3 yields increasing the achievable transmission length increases with 1.5 km, while increasing the number k from 3 to the infinity yields increasing it only with 0.7 km.

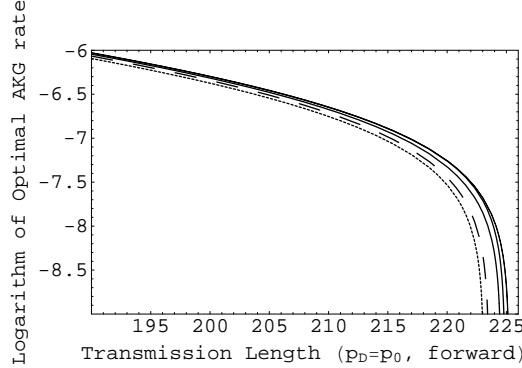


Figure 2. The transmission rate with the forward error correction ($p_D = p_0$): From left to right, (2), (3.2), (3.3), (4), (5)

In order to discuss the reverse error correction case with $p_D = p_0$, we replace the definition of $I(\mu, q^1, b^1)$ as $I(\mu, q^1, b^1) := \frac{1}{2}(\mu e^{-\mu} q^1 (1 - h(\frac{b^1}{q^1})) + p_D - p(\mu)h(s(\mu)))$ in the above table. The transmission rates of the five cases (2), (3.2), (3.3), (4), and (5) with the reverse error correction are given in the Fig 3. The achievable transmission length in the forward case is (2)230.7km, (3.2)231.3km, (3.3)232.5km, (4)233.2km, (5)233.3km. That is, increasing the number k from 2 to 3, yields increasing the achievable transmission length increases with 1.8 km, while increasing the number k from 3 to the infinity

yields increasing it only with 0.8 km. These comparisions indicate that the AKG rate is almost saturated in the case of $k = 3$. Further, these graphs (Figs 1, 2, and 3) show that our AKG rate $\max_{0.3 < \mu_3} I(\mu_3, q_{\min}^{1,3}(0.1, 0.2, \mu_3), b_{\max}^{1,3}(0.1, 0.2, \mu_3))$ is better than Wang's proposal in the case of $k = 3$.

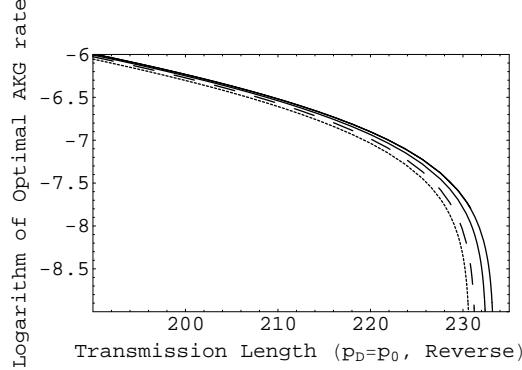


Figure 3. The transmission rate with the reverse error correction ($p_D = p_0$): From left to right, (2), (3.2), (3.3), (4), (5). We cannot distinguish (4) and (5) in this graph.

The optimal signal intensity with the reverse error correction is calculated as Fig 4.

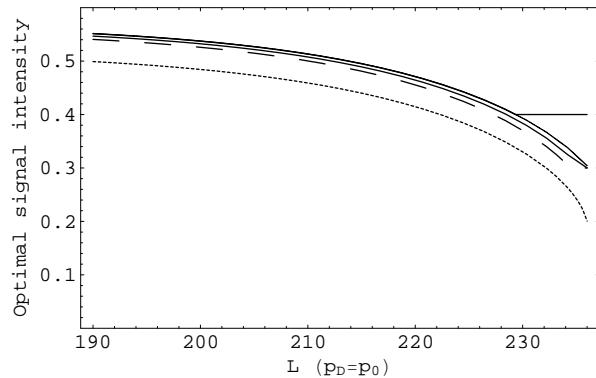


Figure 4. The optimal signal intensity with the reverse error correction ($p_D = p_0$): From up to down, (4), (5), (3.3), (3.2), (2)

8. Proofs of Theorems

8.1. Generalization of the concept “difference”

In this section, in order to prove theorems given in above sections, we generalize the concept of “difference”. In the conventional mean value theorem, we focus on the difference $\frac{f(x_2) - f(x_1)}{x_2 - x_1}$ between two points x_1 and x_2 for a given real-valued function f . When we treat $n+1$ points x_1, \dots, x_{n+1} , we introduce the quantity $\Delta_f^{n+1}(x_1, \dots, x_{n+1}) :=$

$\sum_{i=1}^{n+1} \frac{f(x_i)}{\prod_{1 \leq j \leq n+1, j \neq i} (x_i - x_j)}$ as a generalization of the difference. This generalized difference is characterized by n -th derivative by the following generalization of the mean value theorem:

Lemma 1 Any n -differentiable function f on \mathbb{R} and any $n + 1$ points $x_1 < \dots < x_{n+1}$ satisfy the equation:

$$\Delta_f^{n+1}(x_1, \dots, x_{n+1}) = \frac{1}{n!} \int_{\Delta_n} f^{(n)}\left(\sum_{i=1}^{n+1} a_i x_i\right) p_n(a_1 \dots a_{n+1}) da_1 \dots da_{n+1}, \quad (51)$$

where Δ_n is the n -th simplex, and p_n is the standard uniform probability measure on Δ_n . Hence, there exists a point $z \in [x_1, x_{n+1}]$ such that

$$f^{(n)}(z) = n! \Delta_f^{n+1}(x_1, \dots, x_{n+1}).$$

Its proof will be given in Appendix A. Therefore, the quantity $\Delta_f^{n+1}(x_1, \dots, x_{n+1})$ can be regarded as a generalization of difference. This quantity satisfies the following recurrence formula.

Lemma 2

$$\Delta_f^{n+1}(x_1, \dots, x_{n+1}) = \frac{\Delta_f^n(x_2, \dots, x_{n+1}) - \Delta_f^n(x_1, \dots, x_n)}{x_{n+1} - x_1}. \quad (52)$$

Its proof will be given in Appendix B.

Using this formula, we can prove the following by induction:

$$\Delta_{x^k}^n(x_1, \dots, x_n) = \begin{cases} \sum_{i_l \geq 0: i_1 + \dots + i_n = k-n+1} x_1^{i_1} \cdots x_n^{i_n} & \text{if } k \geq 0 \\ (-1)^{n-1} \sum_{i_l \leq -1: i_1 + \dots + i_n = k-n+1} x_1^{i_1} \cdots x_n^{i_n} & \text{if } k < 0. \end{cases} \quad (53)$$

In particular, when $0 \leq k \leq n-2$,

$$\Delta_{x^k}^n(x_1, \dots, x_n) = 0, \quad (54)$$

which can be also checked by Lemma 1. When $k = -1$, we obtain

$$\Delta_{\frac{1}{x}}^n(x_1, \dots, x_n) = \frac{(-1)^{n-1}}{x_1 \cdots x_n}. \quad (55)$$

For example, when $f(x) = \frac{e^x - e^{(1-\alpha)x} - \alpha x}{x^2}$, the relation (55) yields that

$$\epsilon_\alpha^j(\mu_1, \dots, \mu_j) = (-1)^{j-1} \mu_1 \cdots \mu_j \Delta_f^j(\mu_1, \dots, \mu_j). \quad (56)$$

Since the j -th derivative of x^n is 0 for $n \leq j-1$, the relation (56) holds for $f(x) = \sum_{m=j+1}^{\infty} (1 - (1-\alpha)^m) \frac{x^{m-2}}{m!}$.

Using these formulas, we obtain interesting characterization of the following two $k \times k$ matrixes A_k and B_k :

$$A_{k:i}^l := \begin{cases} \prod_{t=1}^{l-1} (\mu_i - \mu_t) & \text{if } 1 \leq l \leq i \\ 0 & \text{if } i+1 \leq l \end{cases}$$

$$B_{k:l}^i := \begin{cases} \frac{1}{\prod_{t=1, t \neq i}^l (\mu_i - \mu_t)} & \text{if } l \geq i \\ 0 & \text{if } 1 \leq l \leq i-1. \end{cases}$$

That is,

$$\begin{aligned}
A_k &= \begin{pmatrix} A_k^1 & A_k^2 & A_k^3 & \cdots & A_k^k \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & \mu_2 - \mu_1 & 0 & \cdots & 0 \\ 1 & \mu_2 - \mu_1 & \prod_{t=1}^2 (\mu_3 - \mu_t) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \mu_2 - \mu_1 & \prod_{t=1}^2 (\mu_3 - \mu_t) & \cdots & \prod_{t=1}^{k-1} (\mu_k - \mu_t) \end{pmatrix} \\
B_k &= \begin{pmatrix} B_{k:1} \\ B_{k:2} \\ B_{k:3} \\ \vdots \\ B_{k:k} \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ \frac{1}{\mu_1 - \mu_2} & \frac{1}{\mu_2 - \mu_1} & 0 & \cdots & 0 \\ \frac{1}{\prod_{t=1, t \neq 1}^3 (\mu_1 - \mu_t)} & \frac{1}{\prod_{t=1, t \neq 2}^3 (\mu_2 - \mu_t)} & \frac{1}{\prod_{t=1, t \neq 3}^3 (\mu_3 - \mu_t)} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\prod_{t=1, t \neq k}^k (\mu_1 - \mu_t)} & \frac{1}{\prod_{t=1, t \neq 2}^k (\mu_2 - \mu_t)} & \frac{1}{\prod_{t=1, t \neq 3}^k (\mu_3 - \mu_t)} & \cdots & \frac{1}{\prod_{t=1, t \neq k}^k (\mu_k - \mu_t)} \end{pmatrix},
\end{aligned}$$

where A_k^i is the i -th column vector of the matrix A_k and $B_{k:i}$ is the i -th row vector of the matrix B_k .

These matrixes play an important role in the proof of Theorems 1 and 2, and are the inverse matrixes of each other, i.e.,

$$\sum_{i=1}^k B_{k:l}^i A_{k:i}^{l'} = \sum_{i=l'}^l \frac{\prod_{t=1}^{l'-1} (\mu_i - \mu_t)}{\prod_{t=1, t \neq i}^l (\mu_i - \mu_t)} = \delta^{l,l'}, \quad (57)$$

which is equivalent with

$$\sum_{l=1}^k B_{k:l}^i A_{k:i'}^l = \delta_{i,i'}. \quad (58)$$

The equation (57) is trivial in the case of $l' \geq l$. When $l' < l$,

$$\sum_{i=l'}^l \frac{\prod_{t=1}^{l'-1} (\mu_i - \mu_t)}{\prod_{t=1, t \neq i}^l (\mu_i - \mu_t)} = \sum_{i=l'}^l \frac{1}{\prod_{t=l', t \neq i}^l (\mu_i - \mu_t)}. \quad (59)$$

Applying Lemma 1 to the case of $n = l - l' + 1$ and $f(x) = 1$, we can show that LHS of (59) is equal to 0.

Now, we modify the matrix A_k as follows:

$$C_{k:i}^l := \begin{cases} \frac{1}{\mu_i} & \text{if } l = 1 \\ \prod_{t=1}^{l-2} (\mu_i - \mu_t) & \text{if } 2 \leq l \leq i+1 \\ 0 & \text{if } i+2 \leq l. \end{cases}$$

That is,

$$C_k = \begin{pmatrix} \frac{1}{\mu_1} & 1 & 0 & 0 & \cdots & 0 \\ \frac{1}{\mu_2} & 1 & \mu_2 - \mu_1 & 0 & \cdots & 0 \\ \frac{1}{\mu_3} & 1 & \mu_2 - \mu_1 & \prod_{t=1}^2 (\mu_3 - \mu_t) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\mu_{k-1}} & 1 & \mu_2 - \mu_1 & \prod_{t=1}^2 (\mu_3 - \mu_t) & \cdots & \prod_{t=1}^{k-1} (\mu_k - \mu_t) \\ \frac{1}{\mu_k} & 1 & \mu_2 - \mu_1 & \prod_{t=1}^2 (\mu_3 - \mu_t) & \cdots & \prod_{t=1}^{k-1} (\mu_k - \mu_t) \end{pmatrix} = \begin{pmatrix} A_k^0 & A_k^1 & A_k^2 & A_k^3 & \cdots & A_k^{k-1} \end{pmatrix},$$

where

$$A_k^0 = \begin{pmatrix} \frac{1}{\mu_1} \\ \frac{1}{\mu_2} \\ \frac{1}{\mu_3} \\ \vdots \\ \frac{1}{\mu_{k-1}} \\ \frac{1}{\mu_k} \end{pmatrix}.$$

The inverse matrix C_k^{-1} is characterized as follows:

$$C_k^{-1} = \begin{pmatrix} \vec{0}^T \\ B_{k:1} \\ B_{k:2} \\ B_{k:3} \\ \vdots \\ B_{k:k-1} \end{pmatrix} - (-1)^k \begin{pmatrix} \mu_1 \mu_2 \cdots \mu_k B_{k:k} \\ -\mu_2 \mu_3 \cdots \mu_k B_{k:k} \\ \mu_3 \mu_4 \cdots \mu_k B_{k:k} \\ -\mu_4 \mu_5 \cdots \mu_k B_{k:k} \\ \vdots \\ (-1)^{k-1} \mu_k B_{k:k} \end{pmatrix}. \quad (60)$$

The equation (60) can be checked as follows. Using (55), we obtain

$$\mu_1 \mu_2 \cdots \mu_k B_{k:k} A_k^0 = \sum_{i=1}^k (-1)^{k-i} \frac{\mu_1 \cdots \mu_k}{\prod_{t=1, t \neq i}^k (\mu_i - \mu_t)} C_{k:i}^1 = 1,$$

Since

$$B_{k:i-1} A_k^0 = \sum_{l=1}^{i-1} \frac{1}{\mu_l \prod_{t=1, t \neq l}^{i-1} (\mu_l - \mu_t)} = \frac{(-1)^{i-2}}{\mu_1 \mu_2 \cdots \mu_{i-1}}$$

$$(-1)^{k+i} \mu_i \mu_{i+1} \cdots \mu_k B_{k:k} A_k^0 = (-1)^{k+i} \mu_i \mu_{i+1} \cdots \mu_k \frac{(-1)^{k-1}}{\mu_1 \cdots \mu_k},$$

we have

$$(B_{k:i-1} + (-1)^{k+i} \mu_i \mu_{i+1} \cdots \mu_k B_{k:k}) A_k^0 = 0$$

for $k \geq i \geq 2$. Further

$$(B_{k:i-1} + (-1)^{k+i} \mu_i \mu_{i+1} \cdots \mu_k B_{k:k}) A_k^j = B_{k:i-1} A_k^{j-1} = \delta_i^j$$

for $k \geq i \geq 2, k \geq j \geq 2$, and

$$-(-1)^k \mu_1 \mu_2 \cdots \mu_k B_{k:k} A_k^{j-1} = 0$$

for $k \geq j \geq 2$. Thus, we obtain (60).

8.2. Proof of Theorem 1

Now, we prove Theorem 1. First, we check the positivity of ρ_i , which is equivalent with the positivity of $\gamma_{l,n}$ for $i = 2, \dots, k+1$, $n \geq 2$. Substituting $l-2$ and x^{n-2} into n and $f(x)$ in Theorem 1, we have

$$\begin{aligned} (l-2)!\gamma_{l,n} &= (l-2)! \sum_{j=1}^{l-1} \frac{\mu_j^{n-2}}{\prod_{t=1, t \neq j}^{l-1} (\mu_j - \mu_t)} \\ &= \int_{\Delta_{l-2}} \frac{(n-2)!}{(n-l)!} \left(\sum_{t=1}^{l-1} a_t \mu_t \right)^{n-l} p_{l-2}(a_1, \dots, a_{l-1}) da_1 \dots da_{l-1} \geq 0. \end{aligned}$$

The equation (30) is equivalent with

$$\mu_s^2 \sum_{n=2}^{\infty} \frac{\mu_s^{n-2}}{n!} |n\rangle \langle n| = \mu_s^2 \sum_{l=2}^{s+1} \prod_{t=1}^{l-2} (\mu_i - \mu_t) \Omega_l \rho_l$$

Applying (58) to the case of $k = s$, any function f satisfies

$$f(\mu_s) = \sum_{l=1}^s \sum_{j=1}^l \frac{\prod_{t=1}^{l-1} (\mu_s - \mu_t)}{\prod_{t=1, t \neq j}^l (\mu_j - \mu_t)} f(\mu_j).$$

When $f(x) = x^{n-2}$ and $n-2 \leq l-2$, $f^{(l-1)}(x) = 0$. Thus, Theorem 1 yields that

$$\sum_{j=1}^l \frac{1}{\prod_{t=1, t \neq j}^l (\mu_j - \mu_t)} f(\mu_j) = 0.$$

Therefore,

$$\begin{aligned} \sum_{n=2}^{\infty} \frac{\mu_s^{n-2}}{n!} |n\rangle \langle n| &= \sum_{n=2}^{\infty} \sum_{l=1}^s \sum_{j=1}^l \frac{\prod_{t=1}^{l-1} (\mu_s - \mu_t)}{\prod_{t=1, t \neq j}^l (\mu_j - \mu_t)} \frac{\mu_j^{n-2}}{n!} |n\rangle \langle n| \\ &= \sum_{l=1}^s \prod_{t=1}^{l-1} (\mu_s - \mu_t) \sum_{n=l+1}^{\infty} \sum_{j=1}^l \frac{\mu_j^{n-2}}{n! \prod_{t=1, t \neq j}^l (\mu_j - \mu_t)} |n\rangle \langle n| \\ &= \sum_{l=1}^s \prod_{t=1}^{l-1} (\mu_s - \mu_t) \sum_{n=l+1}^{\infty} \frac{\gamma_{l+1,n}}{n!} |n\rangle \langle n| = \sum_{l=1}^s \prod_{t=1}^{l-1} (\mu_i - \mu_t) \Omega_{l+1} \rho_{l+1}, \end{aligned}$$

which implies (30).

8.3. Proof of Theorem 2

Next, we prove Theorem 2. When we fix the parameter q^{1+j} as well as q^0 , the parameters q^1, \dots, q^j are uniquely decided only from the parameters p_1, \dots, p_j . That is, the relation

$$\begin{aligned} \tilde{q}_{j,\min} &:= \min_{\vec{q}=(q^0, \dots, q^{2k+1})^T} \left\{ q^1 \middle| \begin{array}{l} p_i = \sum_{j=0}^{2k+1} P_i^j q^j + p_D \\ 1 - p_D \geq q^{1+j} \geq 0 \end{array} \right\} \\ &= \min_{\vec{q}=(q^0, \dots, q^{j+1})^T} \left\{ q^1 \middle| \begin{array}{l} p_i = \sum_{t=0}^{j+1} P_i^t q^t + p_D \\ \text{for } i = 1, \dots, j \\ 1 - p_D \geq q^{1+j} \geq 0 \end{array} \right\}. \end{aligned}$$

Now, we focus on parameters q^1, \dots, q^{j+1} . Then, we have

$$\begin{aligned} & p_i - p_D - e^{-\mu_i}(p_0 - p_D) \\ &= \sum_{s=1}^j e^{-\mu_i} \mu_i^2 C_{j;i}^s \Omega_s q^s + e^{-\mu_j} \mu_j^2 \prod_{t=1}^{j-1} (\mu_j - \mu_t) \Omega_{j+1} q^{j+1} \delta_{i,j} \end{aligned}$$

for $i = 1, \dots, j$. Using (60) and (41), we have

$$\begin{aligned} q^1 &= \sum_{i=1}^j (C_j^{-1})_1^i \frac{e^{\mu_i}}{\mu_i^2} \left(p_i - p_D - e^{-\mu_i}(p_0 - p_D) - e^{-\mu_j} \mu_j^2 \prod_{t=1}^{j-1} (\mu_j - \mu_t) \Omega_{j+1} q^{j+1} \delta_{i,j} \right) \\ &= \sum_{i=1}^j \beta_i^j \left(p_i - p_D - e^{-\mu_i}(p_0 - p_D) \right) - (-1)^{j-1} \mu_1 \cdots \mu_j \Omega_{j+1} q^{j+1}. \end{aligned}$$

Note that $\Omega_{j+1} \geq 0$. Since $0 \leq q^{j+1} \leq 1 - p_D$, we obtain (42). Similarly, we can prove (43) and (40).

8.4. Proof of Theorem 3

Choose f as $f(x) = \frac{e^x - e^{(1-\alpha)x} - \alpha x}{x^2} = \sum_{n=1}^{\infty} \frac{1}{n!} (1 - (1-\alpha)^n) x^{n-2}$. Using (53) and Lemma 1, we obtain

$$\begin{aligned} & \mu_1 \cdots \mu_j \sum_{n=j+1}^{\infty} \sum_{i_l \geq 0 : i_1 + \cdots + i_j = n-1-j} \frac{1}{n!} (1 - (1-\alpha)^n) \mu_1^{i_1} \cdots \mu_1^{i_j} \\ &= \mu_1 \cdots \mu_j \Delta_f(\mu_1, \dots, \mu_j) \\ &= \mu_1 \cdots \mu_j \sum_{i=1}^j \frac{\sum_{n=1}^{\infty} \frac{1}{n!} (\mu_i^n - ((1-\alpha)\mu_i)^n)}{\mu_i^2 \prod_{1 \leq k \leq j, k \neq i} (\mu_i - \mu_k)} \\ &= \frac{\mu_1 \cdots \mu_j}{(j-1)!} \int_{\Delta_{j-1}} \sum_{n=0}^{\infty} \frac{1 - (1-\alpha)^{n+j+1}}{(n+j+1)(n+j)n!} \left(\sum_{i=1}^j a_i \mu_i \right)^n p_{j-1}(a_1 \dots a_j) da_1 \dots da_j. \end{aligned}$$

Thus, the relations (48) and (49) follow from (56).

Apply (56) to the case of $f(x) = \sum_{m=j+1}^{\infty} \frac{x^{n-2}}{m!}$. We obtain

$$\mu_1 \cdots \mu_j \Omega_{j+1} = \mu_1 \cdots \mu_j \left(\sum_{s=1}^j \frac{\sum_{n=j+1}^{\infty} \frac{\mu_s^{n-2}}{n!}}{\prod_{t=1, t \neq s}^j (\mu_s - \mu_t)} \right) = \epsilon_1^j(\mu_1, \dots, \mu_j),$$

which implies (50).

9. Conclusion and further improvement

We have discussed the AKG rates with phase-randomized coherent light by the decoy method, in which the number k of possible intensities is arbitrary. For this purpose, by generalizing Wang's expansion, we have derived a convex expansion of the phase-randomized coherent state, which allows us to parameterize Eve's operation using $3k+3$ parameters even in the general case. Thanks to this parameterization, lower bound of AKG rate has been obtained with k decoy intensities. Also, assuming that the noise in

the quantum channel is described by a natural model, we have derived upper bounds independent of the number k of decoy intensities as the universal upper bound. It has been numerically demonstrated that the AKG rate is close to the universal upper bound in the case of $k = 3$, i.e., the AKG rates cannot be improved so much even if we prepare a number of intensities k larger than 3.

Further, we have discussed the intensity maximizing our upper bound of the AKG rate. It has been shown that this optimum intensity is always less than 1. We have also characterized the relationship between the AKG rate and intensities that do not generate raw keys. These results indicate how to choose intensities in an implemented quantum key distribution system, in which the decoy method is applied. Unfortunately, this paper does not treat the security with the finite-length code. However, we will treat this issue in the papers [24, 21], in which our expansion (30) and the matrix P_k play an essential role.

For a further improvement of AKG rate, we can assume that some error happens in the generator or the detector. In this case, there is a relation $r^{1'} = (1-p_S)r^1 + p_S(1-r^1)$ between the observed error rate $r^{1'}$ in the \times basis and the error rate r^1 out side of the generator and the detector in the \times basis, where p_S is the probability that the error in the \times basis occurs at generation or detection in the single-photon state. That is,

it is suitable to substitute $\frac{b_{\max}^1 - p_S}{q_{\min}^1 - 1 - 2p_S}$ in side of the binary entropy h . If it is possible to distinguish the error probabilities at generation and detection, a further improvement is available. By taking into account bit error probability among single-photon states at generating the pulse, a tighter evaluation of the AKG rate of the forward case may be possible in a way similar to Renner et al.[25].

Acknowledgments

The author would like to thank Professor Hiroshi Imai of the ERATO-SORST, QCI project for support. He is grateful to Professor Hiroshi Imai, Dr. Akihisa Tomita, Dr. Tohya Hiroshima, and Mr. Jun Hasewaga for useful discussions. He thanks Dr. Francesco Buscemi for his helpful comments.

Appendix A. Proof of Lemma 1

We will prove (51) by induction. The case of $n = 1$ is trivial. By the assumption of induction, we obtain the following equations.

$$\int_{\Delta_{n-1}} f^{(n-1)} \left(\sum_{i=1}^n a_i x_i \right) p_{n-1}(a_1 \dots a_n) da_1 \dots da_n = (n-1)! \sum_{i=1}^n \frac{f(x_i)}{\prod_{1 \leq j \leq n, j \neq i} (x_i - x_j)}, \quad (\text{A.1})$$

$$\int_{\Delta_{n-1}} f^{(n-1)} \left(\sum_{i=2}^{n+1} a_i x_i \right) p_{n-1}(a_2 \dots a_{n+1}) da_2 \dots da_{n+1} = (n-1)! \sum_{i=2}^{n+1} \frac{f(x_i)}{\prod_{2 \leq j \leq n+1, j \neq i} (x_i - x_j)}. \quad (\text{A.2})$$

Thus,

$$\begin{aligned}
& \int_{\Delta_{n-1}} p_{n-1}(a_1 \dots a_n) f^{(n-1)} \left(\sum_{i=2}^{n+1} a_i x_i \right) da_2 \dots da_{n+1} \\
& - \int_{\Delta_{n-1}} f^{(n-1)} \left(\sum_{i=1}^n a_i x_i \right) p_{n-1}(a_2 \dots a_{n+1}) da_1 \dots da_n \\
& = (n-1)! \left(\sum_{i=2}^n \frac{f(x_i) \left(\frac{1}{x_i - x_{n+1}} - \frac{1}{x_i - x_1} \right)}{\prod_{2 \leq j \leq n, j \neq i} (x_i - x_j)} + \frac{f(x_1)}{\prod_{2 \leq j \leq n} (x_1 - x_j)} - \frac{f(x_{n+1})}{\prod_{2 \leq j \leq n} (x_{n+1} - x_j)} \right) \\
& = (n-1)! \left(\sum_{i=2}^n \frac{f(x_i)}{\prod_{2 \leq j \leq n, j \neq i} (x_i - x_j)} \frac{x_{n+1} - x_1}{(x_i - x_{n+1})(x_i - x_1)} \right. \\
& \quad \left. - \frac{f(x_1)}{\prod_{2 \leq j \leq n} (x_1 - x_j)} + \frac{f(x_{n+1})}{\prod_{2 \leq j \leq n} (x_{n+1} - x_j)} \right) \\
& = (n-1)! (x_{n+1} - x_1) \left(\sum_{i=2}^n \frac{f(x_i)}{\prod_{1 \leq j \leq n+1, j \neq i} (x_i - x_j)} + \frac{f(x_1)}{\prod_{2 \leq j \leq n+1} (x_1 - x_j)} + \frac{f(x_{n+1})}{\prod_{1 \leq j \leq n} (x_{n+1} - x_j)} \right) \\
& = (n-1)! (x_{n+1} - x_1) \sum_{i=1}^{n+1} \frac{f(x_i)}{\prod_{1 \leq j \leq n+1, j \neq i} (x_i - x_j)}.
\end{aligned}$$

Now, we introduce new parameters $b = 1 - a_1$ or $1 - a_{n+1}$ and $b_i = \frac{a_i}{b}$ ($i = 2, \dots, n$). Then,

$$\begin{aligned}
& (n-1)! (x_{n+1} - x_1) \sum_{i=1}^{n+1} \frac{f(x_i)}{\prod_{1 \leq j \leq n+1, j \neq i} (x_i - x_j)} \\
& = (n-1) \int_{\Delta_{n-2}} \int_0^1 f^{(n-1)} \left(\sum_{i=2}^n b b_i x_i + (1-b)x_{n+1} \right) db b^{n-2} p_{n-2}(b_2 \dots b_n) db_2 \dots db_n \\
& - (n-1) \int_{\Delta_{n-2}} \int_0^1 f^{(n-1)} \left(\sum_{i=2}^n b b_i x_i + (1-b)x_1 \right) db b^{n-2} p_{n-2}(b_2 \dots b_n) db_2 \dots db_n \\
& = (n-1) \int_{\Delta_{n-2}} \int_0^1 \left(f^{(n-1)} \left(\sum_{i=2}^n b b_i x_i + (1-b)x_{n+1} \right) - f^{(n-1)} \left(\sum_{i=2}^n b b_i x_i + (1-b)x_1 \right) \right) \\
& db b^{n-2} p_{n-2}(b_2 \dots b_n) db_2 \dots db_n \\
& = (n-1)(x_{n+1} - x_1) \int_{\Delta_{n-2}} \int_0^1 \int_0^1 f^{(n)} \left(\sum_{i=2}^n b b_i x_i + (1-b)(x_{n+1} - x_1)s + (1-b)x_1 \right) ds \\
& db (1-b)b^{n-2} p_{n-2}(b_2 \dots b_n) db_2 \dots db_n \\
& = \frac{1}{n} (x_{n+1} - x_1) \int_{\Delta_n} f^{(n)} \left(\sum_{i=1}^{n+1} c_i x_i \right) p_n(b_1 \dots b_{n+1}) dc_1 \dots dc_{n+1} \tag{A.3}
\end{aligned}$$

In equation (A.3), we introduce parameters $c_1 = (1-b)(1-s)$, $c_i = b b_i$ ($i = 2, \dots, n$), $c_{n+1} = (1-b)s$, and use the relation $(1-b)dc_1 dc_{n+1} = dsdb$. The coefficient $\frac{1}{n}$ in (A.3) can be checked by the relation

$$\int_{\Delta_{n-2}} \int_0^1 \int_0^1 dsdb (1-b)b^{n-2} p_{n-2}(b_2 \dots b_n) db_2 \dots db_n = \frac{1}{n(n-1)}.$$

Therefore, we obtain (51).

Appendix B. Proof of Lemma 2

Since $\frac{1}{(x_i-x_1)(x_i-x_{n+1})} = (\frac{1}{x_i-x_{n+1}} - \frac{1}{x_i-x_1})\frac{1}{x_{n+1}-x_1}$, $\Delta_f^{n+1}(x_1, \dots, x_{n+1})$ is calculated as follows:

$$\begin{aligned} & \Delta_f^{n+1}(x_1, \dots, x_{n+1}) \\ &= \frac{1}{(x_i-x_1)(x_i-x_{n+1})} \sum_{i=2}^n \frac{f(x_i)}{\prod_{j=2, j \neq i}^n (x_i - x_j)} + \frac{f(x_1)}{\prod_{j=2}^{n+1} (x_1 - x_j)} + \frac{f(x_{n+1})}{\prod_{j=1}^n (x_{n+1} - x_j)} \\ &= \frac{1}{x_{n+1} - x_1} \sum_{i=2}^n \frac{f(x_i)}{\prod_{j=2, j \neq i}^{n+1} (x_i - x_j)} - \frac{1}{x_{n+1} - x_1} \sum_{i=2}^n \frac{f(x_i)}{\prod_{j=1, j \neq i}^n (x_i - x_j)} \\ &\quad + \frac{1}{x_1 - x_{n+1}} \frac{f(x_1)}{\prod_{j=2}^n (x_1 - x_j)} + \frac{1}{x_{n+1} - x_1} \frac{f(x_{n+1})}{\prod_{j=2}^n (x_{n+1} - x_j)} \\ &= \frac{1}{x_{n+1} - x_1} \Delta_f^n(x_2, \dots, x_{n+1}) - \frac{1}{x_{n+1} - x_1} \Delta_f^n(x_1, \dots, x_n). \end{aligned}$$

Appendix C. Proof of (12) and (13)

It is sufficient to show

$$\frac{dI_{\rightarrow}(\mu; p_0, p_D, p_S, \alpha, s)}{d\mu} \Big|_{\mu=1} \leq 0 \quad (\text{C.1})$$

$$\frac{dI_{\leftarrow}(\mu; p_0, p_D, p_S, \alpha, s)}{d\mu} \Big|_{\mu=1} \leq 0. \quad (\text{C.2})$$

From the assumption, the parameter s' also satisfies $0 \leq s' \leq 1/2$. Hence, $\overline{h}(\frac{s'(1-e^{-\alpha\mu})+\frac{1}{2}p_0}{1-e^{-\alpha\mu}+p_0})$ is monotone increasing concerning μ , i.e., $\frac{d\overline{h}(\frac{s'(1-e^{-\alpha\mu})+\frac{1}{2}p_0}{1-e^{-\alpha\mu}+p_0})}{d\mu} \geq 0$. Since

$$\begin{aligned} & \frac{dI_{\rightarrow}(\mu; p_0, p_D, p_S, \alpha, s)}{d\mu} \\ &= \frac{1}{2} \left((1-\mu)e^{-\mu}(\alpha + (p_0 - p_D))(1 - \overline{h}(\frac{s\alpha + \frac{1}{2}(p_0 - p_D)}{\alpha + (p_0 - p_D)})) \right. \\ &\quad \left. - e^{-\mu}p_0 - (1 - e^{-\alpha\mu} + p_0) \frac{d\overline{h}(\frac{s'(1-e^{-\alpha\mu})+\frac{1}{2}p_0}{1-e^{-\alpha\mu}+p_0})}{d\mu} - e^{-\alpha\mu}\overline{h}(\frac{s'(1-e^{-\alpha\mu})+\frac{1}{2}p_0}{1-e^{-\alpha\mu}+p_0}) \right), \\ & \frac{dI_{\leftarrow}(\mu; p_0, p_D, p_S, \alpha, s)}{d\mu} \\ &= \frac{1}{2} \left((1-\mu)e^{-\mu}(\alpha + (p_0 - p_D))(1 - \overline{h}(\frac{s\alpha + \frac{1}{2}(p_0 - p_D)}{\alpha + (p_0 - p_D)})) \right. \\ &\quad \left. - (1 - e^{-\alpha\mu} + p_0) \frac{d\overline{h}(\frac{s'(1-e^{-\alpha\mu})+\frac{1}{2}p_0}{1-e^{-\alpha\mu}+p_0})}{d\mu} - e^{-\alpha\mu}\overline{h}(\frac{s'(1-e^{-\alpha\mu})+\frac{1}{2}p_0}{1-e^{-\alpha\mu}+p_0}) \right), \end{aligned}$$

we can check (C.1) and (C.2).

References

- [1] C.H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India, IEEE, New York, 1984) 175.
- [2] D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," In *Advances in Cryptology – Proc. Crypto'96, Vol. 1109 of Lecture Notes in Computer Science* (Ed. N. Koblitz, Springer-Verlag, New York, 1996) 343; J. Assoc. Comput. Mach. 48 (2001) 351.
- [3] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," *New J. Phys.*, **4**, 41 (2002).
- [4] T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura, *Jpn. J. Appl. Phys.*, **43**, L1217 (2004).
- [5] C. Gobby, Z. L. Yuan, and A. J. Shields, *Appl. Phys. Lett.*, **84**, 3762 (2004).
- [6] A. Tanaka, W. Maeda, A. Tajima, and S. Takahashi, *Proceedings of the 18th Annual Meeting of the IEEE Lasers and Electro-Optics Society*, Sidney, Australia, 23–27 October 2005, p. 557.
- [7] Z. L. Yuan and A. J. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fiber," *Optics Express*, **13**, 660 (2005).
- [8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quant. Inf. Comput.*, **4**, 325 – 360 (2004).
- [9] H. Inamori, N. Lütkenhaus, and D. Mayers "Unconditional Security of Practical Quantum Key Distribution," quant-ph/0107017.
- [10] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," *Phys. Rev. Lett.*, **91**, 057901 (2003).
- [11] H.-K. Lo, X.-F. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Phys. Rev. Lett.*, **94**, 230504, (2005).
- [12] X.-B. Wang, "Beating the PNS attack in practical quantum cryptography," *Phys. Rev. Lett.*, **94**, 230503 (2005).
- [13] X.-F. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A* **72**, 012326 (2005).
- [14] X.-B. Wang, "A decoy-state protocol for quantum cryptography with four intensities of coherent states," *Phys. Rev., A* **72**, 012322 (2005).
- [15] X.-B. Wang, "Quantum Key Distribution: Security, Feasibility and Robustness," in *Quantum Computation and Information: From Theory to Experiment*, H. Imai and M. Hayashi (eds.), (Springer, Berlin Heidelberg, 2006), pp. 185 – 233; X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," *Physics Reports*, **448**, 1-111 (2007).
- [16] H.-K. Lo, "Getting something out of nothing," *Quant. Inf. Comput.*, **5**, 413 (2005); quant-ph/0503004.
- [17] J.-C. Boileau, J. Batuwantudawe, and R. Laflamme "Higher-security thresholds for quantum key distribution by improved analysis of dark counts," *Phys. Rev., A* **72**, 032321 (2005).
- [18] M. Koashi, "Efficient quantum key distribution with practical sources and detectors," quant-ph/0609180.
- [19] X. B. Wang, *Phys. Rev A* **75**, 012301 (2007) .
- [20] X.-B. Wang, C.-Z. Peng, and J.-W. Pan, *Appl. Phys. Lett.* **90**, 031110 (2007).
- [21] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita, "Security analysis of decoy state quantum key distribution incorporating finite statistics," arXiv:0707.3541.
- [22] M. Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with decoy method," quant-ph/0702250; *Phys. Rev., A* **76** 012329 (2007).
- [23] Oneline at \protect\vrule width0pt\protect\href{http://www.sei.co.jp/fbr-opt-eng/submarine/zplus/pd... \protect\vrule width0pt\protect\href{http://www.corning.com/opticalfiber/products__applications/p...}
- [24] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, "Experimental Decoy State Quantum Key Distribution with Unconditional Security Incorporating Finite Statistics,"

arXiv:0705.3081.

- [25] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols,” *Phys. Rev. A* **72** (2005) 012332, quant-ph/0502064.